		DIRECTIVE			NUMB	ER 920.01			
			DINE		DA	TE <u>2/2/2009</u>	_		
8	FINANCIAL CRIMES ENFORCEMENT NETWORK								
Check one:	Ssuance	Bulletin	🗌 Manual	Supplement	Amendment	🏝 Revision			
SUBJECT: TELEWORK PROGRAM									

1. PURPOSE:

This directive describes the Financial Crimes Enforcement Network's (FinCEN) policy regarding Teleworking workplace arrangements. This program provides an opportunity for an employee to work at an alternate worksite, including an employee's residence, without changing an employee's official duty station or other conditions of employment.

2. POLICY:

FinCEN's policy is to provide all employees the opportunity to participate in the Telework Program when practical and consistent in fulfilling the bureau's mission and meeting its objectives. Telework programs are designed to allow employees to perform their duties at a worksite other than the traditional office setting on an episodic, limited or expanded basis, depending on the organizational mission and the roles and responsibilities of a particular office and its employees.

Participation in the Telework Program is voluntary and subject to first-level supervisory approval, in consultation with the second-level supervisor, based on mission requirements and the efficiency of the Federal service. The Telework Program applies to home or other worksites geographically convenient to the residence of the employee and located in the commuting area of the employee's official duty station.

3. AUTHORITIES:

- A. Federal Employees Clean Air Incentives Act, Pub. L. 103-172 (December 12, 1993).
- B. Public Law 105-277. Omnibus Appropriation Act, Title IV § 630 (October 21, 1998).
- C. Public Law 106-346, § 359. Department of Transportation and Related Agencies Appropriations Act (October 23, 2000).
- D. Treasury Directive 74-14, Treasury Alternative Workplace Arrangements (October 30, 2007).

4. SCOPE:

Participation is limited to FinCEN employees. This policy does not cover detailees, students, platform, or contractor personnel.

5. SUPERSEDED MATERIAL:

l

This directive supersedes FinCEN Directive 920.01, dated 1/30/2006.

6. OFFICE OF PRIMARY INTEREST:

Management Programs Division, Office of Human Resources.

<u>/s/</u> James H. Freis, Jr. Director

TELEWORK PROGRAM

1. PROGRAM DEFINITIONS:

- A. <u>Telework</u> is a voluntary, flexible work arrangement that allows an employee to work away from the traditional office or official duty station at an alternate worksite one or more days per pay period. Telework is also commonly referred to as "telecommuting" and "work-at-home". Telework programs may be designed to allow employees to work at an alternate worksite on an episodic, limited, or expanded basis, depending on the organizational mission and the roles and responsibilities of a particular office and its employees. Telework permits employees to engage in working arrangements at designated locations or other pre-approved alternative worksites known as "flexiplace work environments". Working at an alternate FinCEN worksite is not considered Telework.
- B. <u>Flexiplace work environment</u> refers to an alternative location at which an employee works in lieu of reporting to his/her official duty station. Examples of flexiplace work environments include home sites and telework centers.
- C. <u>Telework center</u> is a General Services Administration facility that provides workstations and other office facilities/services that are used (typically on a fee for use/service basis) by employees from different agencies. Telework centers are equipped with telecommunications and other office equipment to facilitate communication with the official duty station and other places of business in order to perform daily work assignments. Telework centers are not available as an alternate worksite to FinCEN employees and are specifically excluded under this policy.
- D. <u>Remote work</u> is an extension of work that employees may take home to perform on unofficial duty time or work done on temporary duty or travel status. This is not considered Telework.
- E. <u>Episodic participation</u> means approved telework to complete short duration project-type work performed on an occasional, one-time, or irregular basis.
- F. <u>Limited participation</u> means an employee works one to two days per week at an alternate worksite on a regular basis under a set schedule.
- G. <u>Expanded participation</u> means an employee works three or more days per week at an alternate worksite on a regular basis under a set schedule.
- H. <u>Official Duty Station</u> is the official office of assignment. Unless otherwise stated, each employee shall report to and perform his/her duties at this location. All pay, leave, and travel entitlements are based on this location.
- I. <u>Sensitive But Unclassified (SBU) Information</u> is information for which unauthorized access to, or the loss or misuse of would adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under

criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

- J. <u>Law Enforcement Sensitive (LES)</u> is a term used by other agencies and Treasury/bureau law enforcement components for sensitive and case related information and should be treated as SBU.
- K. <u>Bank Secrecy Act (BSA) Information</u> is information contained in reports filed with FinCEN pursuant to its authority under the Bank Secrecy Act, 31 U.S.C. § 5311 <u>et seq</u>. and information concerning whether any particular person or transaction is named or referred to in any such report and if so, information concerning the specific form or type of form in which such person or transaction is named or referred to.

2. PROGRAM PROCEDURES:

- A. <u>Participation</u>. Participation in a telework arrangement is voluntary. It is a management option and not an employee entitlement. An employee may participate in the program if the respective first and second-level supervisors:
 - 1. Decide that the employee's job duties and responsibilities are appropriate for offsite work; and
 - 2. Determine that the employee possesses and maintains performance at the Fully Successful level.
- B. <u>Training and Guidelines</u>. All managers, supervisors, and participating employees must attend telework training and comply with this directive.
- C. <u>Agreement</u>. The telework arrangement under which an employee will perform work must be clearly set forth in a written agreement and signed by the first-level supervisor and employee (FIN040). If there is a change in an existing employee/supervisor Telework arrangement, a new Telework agreement must be initiated. No provisions exist in agreements between employees and supervisors which would preclude management from taking any appropriate disciplinary or adverse action against an employee or supervisor who fails to comply with the provisions of the Telework Program. The Telework Agreement may be terminated at any time by either the supervisor or the employee, with notification that is acceptable to the supervisor. Participation in the program will be terminated if an employee's performance does not meet the expected results (e.g., quality, quantity, timeliness), or other conditions of the telework agreement are not met or violated, or if the telework arrangement fails to benefit organizational needs.
- D. <u>Safe Work Environment</u>. Participating employees are required to inspect their alternate worksite using the attached Home-Office Safety Self Inspection Guidelines and Checklist. They are responsible for maintaining a safe work environment and by signing the Telework Program Agreement (Fin040) they certify that they have inspected their alternate worksite and that it is free of significant safety problems.

- E. <u>Conditions of Employment</u>. A telework arrangement does not alter the terms and conditions of employment, including an employee's official duty station, salary, benefits, individual rights, or obligations. All pay, leave, and travel entitlement shall be based on the official duty station. The telework arrangement shall not affect other conditions of employment, e.g., hours of work, time and attendance policies, dismissals, emergency closings, leave or compensation unless otherwise specified in the Telework Program Agreement (Fin040).
- F. <u>Renewal</u>. Participants continuing in either limited or expanded teleworking arrangements after a one-year period must complete an annual Telework Renewal Agreement (FIN042). Before signing the renewal, the first-level supervisor and employee should reassess the arrangement and make sure that there have not been any changes to the criteria and terms of the original Telework Program Agreement (Fin040). If changes to the original arrangement exist (e.g., telework days, alternate worksite address, computer access, etc.), a renewal form should not be signed and a new Telework Agreement (Fin040) should be executed.
- G. <u>Denial</u>. If an employee disputes the reason(s) given by a supervisor for not approving him or her for telework, or for terminating his or her telework agreement, the employee may submit a grievance in accordance with the procedures set forth in Directive 950.03: Administrative Grievance System. The management official's decision in response to the grievance is final.

3. PROGRAM RESPONSIBILITIES:

- A. <u>Senior Management</u>. Management will:
 - 1. Evaluate the impact of the telework program on the efficiency and effectiveness of their work operations.
 - 2. Incorporate teleworking into the Continuity of Operations Plans and Procedures as another alternative for relocating employees to continue providing customer service and carrying out the mission during an emergency situation.
- B. <u>First Level Supervisors</u>. First-level supervisors are responsible for employees under their charge. In this regard, these supervisors, in consultation with their second-level supervisor, will:
 - 1. Ensure the work of the office is accomplished.
 - 2. Ensure that teleworking does not burden staff remaining in the office through an inequitable distribution of workload.
 - 3. Review and approve, or disapprove, employee requests to Telework.
 - 4. Retain the original agreement for their files and forward a copy to the Telework Coordinator, Management Programs Division (MPD), Office of Human Resources.

- 5. Properly certify, approve, and monitor time and attendance for employees working in a telework status including ensuring that employees comply with all overtime and compensatory time off rules.
- 6. Reserve the right to require employees to report to the official duty station on scheduled telework days, based on operational requirements.
- 7. Assign appropriate work to be performed at the alternate worksite, and be accountable for the employee's work as in a regular office setting.
- 8. Maintain performance management records and other appropriate information.
- 9. Enforce safety and security policies affecting the mission of FinCEN in telework activities.
- 10. Attend supervisory telework training before approving telework agreements.
- C. <u>Employees</u>. Employees will complete the Telework Program Agreement (FIN040) and comply with all applicable provisions of the Agreement and this directive. Additionally, employees agree they will:
 - 1. Dedicate official duty time at the alternate worksite to government business only, and shall not treat it as an opportunity to conduct personal business or accommodate child or elder care needs.
 - 2. Be available to respond immediately to unexpected tasking or exigent circumstances during scheduled duty hours, including reporting to the official duty station on scheduled telework days, based on operational requirements, when requested by the supervisor.
 - 3. Observe existing time and attendance policies in requesting leave, overtime, compensatory time, or working an approved Alternate Work Schedule (AWS), and not work overtime or compensatory time off hours unless approved in advance in accordance with procedures.
 - 4. Perform a home-office safety self-inspection using the attached Home-Office Safety Self Inspection Guidelines and Self-Certification Safety Checklist prior to participating in teleworking and monitor the alternate worksite accordingly as conditions may change.
 - 5. Maintain a workspace that is free from personal distractions and safety hazards, and immediately report any on-the-job injuries to the first-level supervisor.
 - 6. Protect government property (equipment and software) from possible theft and environmental damage and ensure that work information in both hard copy and electronic format has been adequately secured. In cases of damage to unsecured equipment by non-employees, the employee will be held liable for repair or replacement of the equipment or software in compliance with applicable regulations on negligence.

- 7. Use Government equipment only for its authorized purposes, complying with FinCEN Directive 303.04, Limited Personal Use of Government Information Technology (IT) Resources.
- 8. Observe all rules, policies, and procedures regarding security, including:
 - a. Be responsible for notifying and coordinating any movement of computer equipment at their telework site with their first level-supervisor and the Technology Solutions and Services Division (TSSD).
 - b. Be required to securely transport their laptops and peripheral devices to the official duty station when in need of repair and upgrade.
 - c. Ensure that the alternate worksite has adequate physical and environmental security measures in place to protect the equipment from being accessed by unauthorized individuals.
 - d. Keep secure any security information such as a secure identification token and password.
 - e. Immediately report any unauthorized or suspicious activity at the alternate worksite using the same protocols as if they were located at their official worksite. Refer to the FinCEN policy on Incident Response and Reporting for further guidelines. (See Directive 804.01, FinCEN Information Technology Security Program, Attachment ISSP – 006.0).
 - f. Information contained on government systems or media will not be transferred or copied to an individually owned personal computer or media (e.g., backup tape, CD, etc.).
 - g. Information contained on a personal computer or media will not be transferred or copied to government systems or media.
- 9. Report suspected computer operational and security problems (i.e., system intrusion attempts, virus warnings, potential information compromises, etc.) to the Service Desk at (703) 905-3767 and to the FinCEN Computer Security Incident Response Capability (CSIRC) point of contact. Refer to the FinCEN policy on Incident Response and Reporting for further guidelines.
- 10. Take training and be certified by TSSD to enable the employee to troubleshoot common problems and move and reconnect IT equipment as necessary at the alternate worksite.
- 11. Teleworking will only be via high speed internet connection (e.g., FIOS, DSL, or cable).
- 12. Attend telework training prior to completing both the Remote Access Agreement (FIN039) and the Telework Program Agreement (FIN040).
- D. <u>Technology Solutions and Services Division (TSSD)</u>. In addition to standard organizational responsibilities, FinCEN has the right to inspect, during normal work hours with 24 hours of notice to the employee, the alternate worksite and government furnished equipment to monitor safety and security conditions. The proposed technology support will be provided based on the following framework:

- 1. Due to the sensitive nature of FinCEN's mission, all information will be handled at a heightened level of security awareness critical to maintain a safe and secure telework environment. In accordance with TD P 85-01, *Treasury Information Technology Security Program, Volume II, Handbook: Part 1, Sensitive Systems,* Section 5.4.1, the following criteria must be met to ensure the security of the FinCEN network and the data contained therein:
 - a. No classified information will be allowed at the alternate worksite under any circumstance.
 - Employees shall not remove or transfer any SBU, LES, or BSA information from any FinCEN controlled facility to an alternative worksite. Any exceptions to this policy must be approved by the Office of Security. In the event the alternate worksite is approved for and will contain any SBU, LES and/or BSA information, all such information must be kept secured at all times. The Office of Security will provide a security briefing and requirements for the protection, storage, and safeguards for the information outside FinCEN controlled facilities.
 - c. Access to BSA databases will only be through the FinCEN network connection. Access to Law Enforcement databases at alternate worksites is prohibited. All work will be saved on a network drive when connected to the FinCEN network. **Printing and/or downloading any SBU, LES or BSA information at the alternate worksite is strictly prohibited.**
 - d. To properly secure FinCEN's data for teleworking purposes, the following procedures, along with hardware and infrastructure requirements will be initiated:
 - (1) All teleworkers will complete the training and sign a Telework Agreement (FIN040) which must be approved by the individual's supervisor;
 - (2) All teleworkers will complete the requirements for Remote Access to the FinCEN network. This includes the completion of the Remote Access Agreement (FIN039) and all associated training;
 - (3) All teleworkers will be provided a laptop that will be secured by a personal firewall, anti-virus software, full disk encryption, and will be hardened with the requirements set forth in the Federal Desktop Core Configuration (FDCC) security settings; and
 - (4) All teleworkers will utilize the secure Virtual Private Network (VPN) to access the FinCEN network from the FinCEN provided laptop.
- 2. FinCEN TSSD will issue all required equipment to teleworkers. Issuance of government owned IT equipment to the teleworker allows FinCEN to maintain control over the software that resides on the equipment, what security protection is installed on the equipment, and the types of equipment that need to be supported by the TSSD Service Desk.

- 3. The issuance of IT equipment will be based on the teleworker's work requirement. For the purpose of IT support, teleworkers fall into one of two categories:
 - a. <u>Limited or Expanded participation</u> –Each employee engaging in this type of telework will be issued a FinCEN laptop equipped to provide remote access to the FinCEN network.
 - b. <u>Episodic participation</u> Each employee engaging in this type of telework will be able to check out a laptop for use during the period required to complete the task.
- 4. The employee must use his/her own Internet Service Provider (ISP) for connectivity to the FinCEN network. This connection will be through a Digital Subscriber Line (DSL), a cable modem, or through a Fiber Optic Service (FIOS) connection. The connection to the laptop must be direct, that is, via an appropriate network cable. Connecting to the FinCEN network using the laptop's wireless capability or using a wireless air card is not authorized unless approved by TSSD for special circumstances such as international travel.
- 5. FinCEN services available to teleworkers include:
 - a. The Service Desk will furnish and maintain all government owned IT equipment to include loading all required government owned software on the device.
 - b. The Service Desk staff will be available to provide assistance with remote access issues during normal weekday working hours. The Service Desk support hours are from 6:30 AM to 8:00 PM Monday through Friday, Eastern Standard/Daylight Time.
- 6. The limited or expanded participation teleworker may be required, on a periodic basis, to return his/her FinCEN provided laptop to the Service Desk for updates. These updates may include security patches, updated software revisions or new approved software applications. The teleworker will be required to participate in these recalls or remote access may be terminated.
- E. <u>Office of Security</u>. In addition to standard organizational responsibilities, FinCEN has the right to inspect, during normal work hours with 24 hours of notice to the employee, the alternate worksite and government furnished equipment to monitor safety and security conditions.
- F. <u>The Management Programs Division</u> is responsible for policy, general oversight, and program evaluation conducted through the Telework Coordinator. Success of the program depends on a close working relationship between the first-level supervisors and participating employees. The Telework Coordinator may request additional data as determined by the Director of FinCEN, the Department of the Treasury, or the Office of Personnel Management.

4. **REVOCATION OF THE TELEWORK PROGRAM:** The Director or Deputy Director may terminate the Telework Program for any or all positions or job series at any time.

The following information can be applied to any alternative work arrangement, either at a telecenter or at a home office. It is provided to assist you in designing, establishing, adjusting, and/or inspecting your workstation at the alternate worksite. An adequate workstation should be safe and comfortable and should facilitate your job performance.

The following guide will familiarize you with many of the desirable aspects as well as hazards in an office work environment. If you suspect that something is hazardous, but are not sure, you can contact the Bureau Safety and Health Officer for assistance. It is recommended that you maintain this Guide as a reference source.

WORKING OR WALKING SURFACES

Surfaces should be level and free of tripping, bumping, or slipping hazards. Things to look for include: torn carpet; electrical or telephone cords in walkways; partition support brackets, waste baskets, portable heaters, fans, etc. placed in walkways; file cabinet drawers and/or bookcase doors that open into an aisle; misaligned furniture; temporary or permanent storage that narrows or obstructs aisles; doors that open into aisles or narrow halls, etc.

ELECTRICAL SAFETY

There are numerous safety considerations involved in the use of electrically powered equipment and appliances. These center around three hazards - shock, burns, and fire.

Grounding: Generally most homes/buildings are provided with three wire grounded electrical outlets. These should be checked for correct wiring and adequacy of grounds by the owner and/or appropriate officials. You should look for cracked or broken outlets, missing covers which expose the wiring or signs of arcing or burns around the outlet.

The subject of grounding for office type equipment is difficult to cover in this amount of space. As a general rule, if an appliance comes from the manufacturer with a three prong plug, the ground pin should not be broken off nor should the device be used ungrounded via a two prong adapter or extension cord. Large appliances such as refrigerators, computers, paper copiers, etc., as well as heating devices such as coffee pots, hot plates, etc., should be grounded.

Electrical Cords: Appliance and equipment cords should be checked for proper connection to the device, frayed or damaged insulation, defective plug, and exposed wires on a

regular basis. The use of extension cords in the workplace should be limited and closely controlled. Extension cords are to be used only on a "temporary basis." If the condition where they are used calls for "long term use," then electrical outlets should be moved, added, or whatever proper corrective action may be necessary.

Try rearranging the furniture or adding additional electrical outlets before using extension cords. When they are used, they should be of the same or larger wire size as the cord being extended, and have a compatible connector plug. If an adapter is needed to connect the device to an extension cord, the wrong extension cord is being used.

CAUTION: Extension cords must never be draped over furniture, partitions, equipment, etc., or extended across aisles or walkways, nor extended through doors, walls, ceiling, etc., and never located under carpeting.

Electrical Outlets: A major cause of fire is overloaded electrical circuits.

Fire Extinguishers: Are there enough of the proper type of fire extinguishers and are they properly positioned? Fire extinguishers should be permanently mounted. The location of fire extinguishers must be clearly marked. If the view of an extinguisher is obstructed by partitions, furniture, corners, etc., then a directional arrow fire extinguisher location sign or some kind of marking is needed. The access to a fire extinguisher should never be blocked, even temporarily. The travel distance to reach an extinguisher should not exceed 75 feet.

All fire extinguishers should be checked regularly and inspected at least annually. They must have a tag attached showing the inspection date. Fire extinguishers must be hydrostatically tested every five to twelve years. Look for a metal tag or decal showing the last test date. If the extinguisher has a gauge, check to see that it is "full." Usually, this means that the gauge's arrow/needle is pointing straight up. Examine the fire extinguisher's hose and discharge nozzle for damage. Also check to see that the handle locking pin, or wire is intact. If not, the extinguisher could have been used and now has to be refilled. If the extinguisher has any damage, especially surface damage such as dents, or has been discharged or tampered with, it must be inspected again by a qualified person.

Sprinkler Systems: Some facilities have automatic sprinkler protection. If your alternate work area has this, check to see that the sprinkler heads have not been painted. Paint can

clog the sprinkler head and prevent it from operating properly. Storage under and around sprinkler heads should be limited to no closer than 18 inches in any direction to allow ample clearance for the water spray. Do not permit anything to be attached to or suspended from a sprinkler head. Ideally, the sprinkler system should be tied into the building's fire alarm system so that when a sprinkler head is activated, the proper authorities are notified immediately.

STORAGE

The storing of any item on top of tall furniture or cabinets should be prohibited. To permit this practice sets the stage for many types of injuries. Employees attempting to place things on top of furniture or cabinets can strain themselves, can fall if chairs are used in place of ladders or even if ladders are used incorrectly. The items themselves can fall, striking employees. It is best to limit storage to designated storage rooms/areas.

A good practice is to limit storage height to maintain a minimum of 18 inches clearance from the ceiling in general, and from light fixtures and other electrical equipment in particular. If sprinkler protection is provided in the work or storage room, maintain as much clearance between stored items and the sprinkler head as possible; again, 18 inches is a good minimum clearance. Check to see that heavy items are stored on lower shelves. Have a ladder or approved step stool available so you can safely reach high places within the work or storage area.

HEATERS

Care should be exercised when using portable heaters. Be sure that the heating element is guarded against accidental contact, positioned not too close to furniture or other combustibles, and that a tip-over switch cuts off electrical power to the heating element if the heater is knocked over. This feature could prevent the heater from starting a fire. Kerosene heaters should not be used in the work area.

COFFEE POTS OR SIMILAR ITEMS

Use of coffee pots and similar items in the immediate work area should be placed out of normal walk areas and on a

noncombustible surface. Never place such a device in a storeroom, closet, or other location where it cannot be observed. If the device is in a location where it cannot be observed, it could smolder, start a fire and spread beyond control before being detected. Should an electrical shortcircuit occur, quick action is necessary to prevent fires.

THE DESK

The height of the work surface should be comfortable for typical uses (computer work, writing, or reading). Conventional desk surfaces are usually about 29 inches high, which is adequate for many tasks. The height recommended for a computing surface is approximately 26 inches.

THE CHAIR

The chair is probably the most important piece of furniture in your work station. The seat should be adjustable, and the height (measured from the floor) of the top surface of the seat should be 15 to 21 inches. The backrest should be adjustable (height and angle) and should provide support for the teleworker's lower back. Armrests should be substantial enough to provide support, but not so large as to be in the way.

LIGHTING

The lighting in your workstation can affect comfort, visibility, and performance. Whether you're using natural daylight or artificial lighting, it should be directed toward the side or behind your line of vision, not in front or above it. Bright light sources can bounce off working surfaces and diminish your sense of contrast. Northern daylight is the best light for your workstation and for operating a computer.

NOISE

Depending on your personality and work style, noisy or totally noise-free environments can be distracting and stressful. Some background sound such as music can be beneficial in maintaining a level of productivity and reducing boredom.

SELF-CERTIFICATION SAFETY CHECKLIST FOR HOME-BASED TELEWORKERS

A. WORKPLACE ENVIRONMENT

1. Are temperature, noise, ventilation, and lighting levels adequate for maintaining your normal level of job performance?	Yes	_ No
2. Are all stairs with 4 or more steps equipped with handrails?	Yes	_ No
3. Are all circuit breakers and/or fuses in the electrical panel labeled as to intended service?	Yes	No
4. Do circuit breakers clearly indicate if they are in the open or closed position?	Yes	No
5. Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires to the ceiling)?	Yes	No
6. Will the building's electrical system permit the grounding of electrical equipment?	Yes	No
7. Are aisles, doorways, and corners free of obstructions to permit visibility and movement?	Yes	No
8. Are file cabinets and storage closets arranged so drawers and doors do not open into walkways?	Yes	No
9. Do chairs have any loose casters (wheels)?	Yes	No
10. Are the rungs and legs of the chairs sturdy?	Yes	_ No
11. Are the phone lines, electrical cords, and extension wires secured under a desk or alongside a baseboard?	Yes	No
12. Is the office space neat, clean, and free of excessive amounts of combustibles?	Yes	No
13. Are floor surfaces clean, dry, level, and free of worn or frayed seams?	Yes	No
14. Are carpets well secured to the floor and free of frayed or worn seams?	Yes	No
15. Is there enough light for reading?	Yes	No
B. COMPUTER WORKSTATION (IF APPLICABLE)		
1. Is your chair adjustable?	Yes	No
2. Do you know how to adjust your chair?	Yes	No
3. Is your back adequately supported by a backrest?	Yes	_ No
4. Are your feet on the floor or fully supported by a footrest?	Yes	No
5. Are you satisfied with the placement of your VDT and keyboard?	Yes	No
6. Is it easy to read the text on your screen?	Yes	No
7. Do you need a document holder?	Yes	No
8. Do you have enough leg room at your desk?	Yes	No
9. Is the VDT screen free from noticeable glare?	Yes	_ No
10. Is the top of the VDT screen eye level?		_ No
11. Is there space to rest the arms while not keying?		No
12. When keying, are your forearms close to parallel with the floor?	Yes	No
13. Are your wrists fairly straight when keying?	Yes	No